安天发布《DoppelPaymer 勒索软件变种分析报告》

近日，安天 CERT 在梳理网络安全事件时发现一个名为 DoppelPaymer 的勒索软件变种，DoppelPaymer 勒索软件最早于 2019 年 6 月被发现，主要通过 RDP 暴力破解和垃圾邮件进行传播，邮件附件中带有一个自解压文件，运行后释放勒索软件程序并执行。DoppelPaymer 勒索软件与 INDRIK SPIDER 组织的 BitPaymer 勒索软件在部分代码段、勒索信内容和支付赎金网页较为相似，故怀疑 DoppelPaymer 勒索软件隶属于 INDRIK SPIDER 组织。

自解压文件运行后在 %Users% 目录下创建 gratemin 文件夹，释放名为 p1q135no.exe 的勒索软件程序并执行，加密文件后，在原文件名后追加名为“.locked”的后缀，并在每个被加密文件的目录中创建名为原文件名后追加“.readme2unlock.txt”格式的勒索信，勒索信中包含勒索说明、TOR 下载地址、支付地址、data 数据信息和邮箱联系方式等。DoppelPaymer 勒索软件变种使用“RSA+AES”算法加密文件，利用多线程快速加密文件，使用命令 arp －a 以解析受害系统的地址解析协议（ARP）表，调用命令行命令来防止受害者恢复已加密的文件，具体操作为删除卷影副本、禁用修复、删除本地计算机的备份目录等。目前被加密的文件在未得到密钥前暂时无法解密。

安天提醒广大用户，及时备份重要文件，且文件备份应与主机隔离；及时安装更新补丁，避免一切勒索软件利用漏洞感染计算机；对非可信来源的邮件保持警惕，避免打开附件或点击邮件中的链接；尽量避免打开社交媒体分享的来源不明的链接，给信任网站添加书签并通过书签访问；避免使用弱口令或统一的口令；确保所有的计算机在使用远程桌面服务时采取 VPN 连接等安全方式，如果业务上无需使用远程桌面服务，建议将其关闭；可以使用反病毒软件（如安天智甲）扫描邮件附件，确认安全后再运行。

目前，安天追影产品已经实现了对该类勒索病毒的鉴定；安天智甲已经实现了对该勒索病毒的查杀。

木马程序

安天【追影威胁分析系统】无需更新病毒库，即可实现对上述木马程序进行有效检测，下为其自动形成的分析报告：

文件由页面手工提交，经由 BD 静态分析鉴定器、YARA 自定义鉴定器、来源信息鉴定器、数字证书鉴定器、元数据信息鉴定器、字符串分析鉴定器、反病毒引擎鉴定器、动态（WinXP）鉴定器、聚类分析鉴定器、关联分析鉴定器、智能学习鉴定器、静态特征检测鉴定器、安全云鉴定器、信标检测鉴定器、动态（Win7 x86）鉴定器等鉴定分析。

最终依据 BD 静态分析鉴定器、关联分析鉴定器、反病毒引擎鉴定器将文件判定为木马程序。

◆ 概要信息

文件名	f658ddcf8e87de957a81bb92d44ce02913b427e8bccbe663669ee2613d355555
文件类型	BinExecute/Microsoft.EXE[:X86]
大小	3.24 MB
MD5	8C54BBE3F191A8627BFEEB4CB02634A9
病毒类型	木马程序
恶意判定 / 病毒名称	Trojan[Ransom]/Win32.Encoder
判定依据	反病毒引擎

◆ 操作系统

操作系统	内置软件
WinXP 5.1.2600 Service Pack 3 Build 2600	默认、IE6、Firefox、Google Chrome、Office 2003、Flash、WPS、FoxitReader、Adobe Reader

◆ 常见行为

行为描述	危险等级
加载运行时 DLL	★
获取系统版本	★
获取系统信息（处理器版本、处理器类型等）	★
创建窗口	★
打开自身进程文件	★
读取自身	★★
获取当前激活的窗口	★★
查找窗口	★
获取键盘状态	★
获取驱动器类型	★
获取驱动加载权限	★
……	……

◆完整报告地址

安天周观察
安天官方微博 安天官方微信
主办：安天 2019年11月25日(总第209期)试行 本期4版 微信搜索：antiylab 内部资料 免费交流

安天圆满完成进博会网络安保任务

2019 年 11 月 10 日，为期 6 天的第二届中国国际进口博览会在上海国家会展中心圆满落下帷幕，共计 181 个国家、地区、国际组织与会，3800 多家企业参展。本届进博会累计意向成交 711.3 亿美元，比首届增长 23%。

在此期间，安天在网络安全主管部门的统一部署下，圆满完成了本届进博会及相关活动的网络安全保障工作，获得了主管部门的认可。

作为网络安全国家队，安天是本届进博会的网络安全保障工作支撑单位之一。在执行任务期间，安天持续监测安全威胁状态，密切关注关键信息基础设施、信息系统和网站安全运行状况，随时进行风险排查、研判上报和应急处置，保证 7*24 小时实时监测和应急处置，高质高效完成技术检测，有效保障重点目标的网络安全。


感谢信

安天安服团队致力于为客户提供专业的安全服务，帮助用户发现网络安全风险，处置网络安全威胁，提供专业的解决方案。安全服务内容包含安全咨询类、监测分析类、安全评估类、应急保障类等专业服务。安天连续六届蝉联国家级网络安全应急服务支撑单位，是中国应急响应体系中重要的企业节点。安天曾承担十八大、十九大、北京奥运会、上海世博会、北京 APEC、杭州 G20 峰会、一带一路高峰论坛、金砖国家峰会、建国七十周年等重大活动安保，由于安保工作表现突出，多次收到国家有关部门发来的感谢信。未来，安天将继续坚持自主创新、追求能力先进，不断为客户创造价值。

Lazarus 组织使用 Mac 后门攻击韩国用户

趋势科技研究人员发现归属于 Lazarus 组织的 Mac 后门变种，其被用于针对韩国用户。该恶意样本使用带有嵌入式宏的 Excel 文档，宏将仅运行一个 PowerShell 脚本，该脚本连接到该组织设置的三台 C & C 服务器。除了样本外，研究人员还发现了与该攻击有关的 Mac 应用程序捆绑包，它与恶意电子表格共享相似的 C & C 服务器。

（原文链接：https://blog.trendmicro.com/trendlabs-security-intelligence/mac-backdoor-linked-to-lazarus-targets-korean-users/）

安全厂商发布 Jigsaw 勒索软件解密程序

Emsisoft 发布了针对 Jigsaw 勒索软件的新解密程序。Jigsaw 勒索软件不仅会对文件进行加密，还会定时删除它们。在数据加密后的一个小时内删除一个文件，此后每小时删除的文件数量呈指数增长。72 小时后，删除所有剩余文件。如果受害者重新启动或终止勒索软件的进程，它将自动重新启动并删除 1000 个文件。Jigsaw 的解密程序于 2016 年发布。由于该勒索软件已经是开源的，这使得攻击者可以创建多个无法解密的变体。新解密工具目前可以解密 85 个扩展，并将随着新变种的出现而更新。

（原文链接：https://blog.emsisoft.com/en/34636/emsisoft-releases-new-decryptor-for-jigsaw-ransomware/）

研究人员发现针对多平台的后门 ACBackdoor

Intezer 研究人员发现一个新 Linux 后门及其 Windows 变种，并将其称为 ACBackdoor。ACBackdoor 提供 shell 命令的任意执行、任意二进制执行、持久性和更新功能。Linux 二进制文件是静态链接的 ELF 文件，而 Windows 二进制文件是动态链接的 PE 文件。就整体功能而言，该后门的两个实例在本质上是相同的，只是存在实现上的细微差别。二者共享相同的协议以与同一台 C & C 服务器通信，但是具有不同的 传递向量，Windows 实例是通过 Fallout 漏洞利用工具包投送，而 Linux 实例目前未知，这一发现表明，ACBackdoor 背后的攻击组织有足够的资金来购买 Fallout 漏洞利用工具包，并且正在使用它通过恶意广告活动来传播 Windows 版本的后门。目前还未发现该后门与其他威胁组织具有任何已知联系。

（原文链接：https://www.intezer.com/blog-acbackdoor-analysis-of-a-new-multiplatform-backdoor/）

每周安全事件

类 型	内 容
中文标题	虚假 Windows 更新邮件传播 Cyborg 勒索软件
英文标题	Fake Windows Update Spam Leads to Cyborg Ransomware and Its Builder
作者及单位	Diana Lopera
内容概述	Trustwave 研究人员发现通过虚假的 Windows Update 垃圾邮件传播 Cyborg 勒索软件的活动。垃圾邮件声称来自微软的电子邮件，附件为“最新的关键更新”。附件文件扩展名为 ".jpg"，但它实际为可执行文件，此可执行文件是一个恶意的 .NET 下载程序，点击后，将从 Github 下载最终的有效载荷，该文件名为 bitcoingenerator.exe，包含在其 btcgenerator 存储库中，但其实际为 Cyborg 勒索软件。Cyborg 加密的文件名称在原文件名称的基础上加上扩展名“.777”，勒索信要求用户支付 500 美元的比特币。
链接地址	https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/fake-windows-update-spam-leads-to-cyborg-ransomware-and-its-builder/

每周值得关注的恶意代码和漏洞信息

经安天【CERT】检测分析，本周有 8 个移动平台恶意代码和 6 个 PC 平台的恶意代码值得关注

恶意代码类别		名称与发现时间	威胁等级	简要描述
移动恶意代码	新出现的样本家族	Trojan/Android.Joker2.b[prv,pay,exp] 2019-11-17	高	该应用程序包含恶意代码，运行后联网下载恶意子包，解析控制命令，静默模拟点击广告，订阅付费业务，窃取用户短信、联系人列表和设备信息。造成用户隐私泄露和经济损失，建议立即卸载。
		Trojan/Android.Venus121Spy.b[prv,spy] 2019-11-18	中	该应用程序是一款间谍软件，伪装正常应用，运行后加载钓鱼界面，诱导用户填写 Kakao 或 Naver 的账号进行注册，私自替换用户账号登入风险账号，并将用户隐私上传至服务器。造成用户隐私泄露，建议卸载。
		Trojan/Android.HiddenApp.cq[exp,rog] 2019-11-19	低	该应用程序伪装为正常应用，运行隐藏图标，加载推广页面，造成用户的资费消耗，建议卸载。
	较为活跃样本	Trojan/Android.SmsSpy.cl[prv,exp]	中	该应用程序伪装成其他应用，运行监听用户短信并发送到指定号码，造成用户隐私泄露和资费损耗，建议卸载。
		Trojan/Android.InfoStealer.bj[prv]	中	该应用程序包含风险代码，联网上传固件信息，访问指定网页，监听短信通知栏，隐藏通知消息、上传短信内容，会造成用户隐私泄露，请卸载。
		RiskWare/Android.Reshare.a[fra]	低	该应用程序重打包正常应用，增加分享推广页面诱导用户加 QQ 或加群，存在一定的风险，建议谨慎使用。
		G-Ware/Android.HiddenAds.jq[exp,rog]	低	该应用程序伪装为游戏类应用，运行隐藏图标、加载广告，后台推广加载网页，造成用户资费损耗，建议卸载。
		G-Ware/Android.Dropper.dr[rog]	低	该应用程序包含风险代码，私自联网获取配置信息，动态加载未知文件，可能会造成用户资费损耗，请卸载。
PC 平台恶意代码	活跃的格式文档漏洞、0day 漏洞	Windows Hyper-V 远程代码执行漏洞（CVE-2019-1389）	高	当主机服务器上的 Windows Hyper-V 网络交换机无法正确验证来宾操作系统上已通过身份验证的用户输入时，会触发远程代码执行漏洞。攻击者可以在来宾操作系统上运行经特殊设计的应用程序来利用此漏洞，从而执行任意代码。
	较为活跃样本	Trojan[Banker]/Win32.Tuhkit	中	此威胁是一种以窃取网络银行敏感信息（如银行账号、密码、信用卡信息等）为目的的木马类程序。该家族通过恶意网站或已被感染的邮件进行传播。该家族可以监控用户的网络行为，在用户登陆银行网站时记录用户信息，并将所有收集的信息发送给黑客。
		Trojan/Win32.Kolweb	中	此威胁是一种具有多种恶意行为的木马家族。该家族病毒会开机自启，将恶意代码和冗余文件添加到计算机中，导致系统速度变慢甚至崩溃，重定向网页。该家族也会捆绑其他恶意软件并安装。
		Trojan[Ransom]/MSIL.Sram	中	此威胁是一种可以加密用户文件的木马类程序。该家族样本运行后遍历磁盘，加密特定格式的文件并勒索比特币。
		Trojan/MSIL.IObit	低	此威胁是一种使用 MSIL 中间语言编写的木马程序。该家族通常会安装并运行广告件程序，窃取用户信息并回传。
		Trojan/Win32.StartPage	低	此威胁是一种会修改用户浏览器主页并推送广告的木马类家族。

可见性对于增强网络防御至关重要

Craig Harber/ 文 安天技术公益翻译组 / 译

互联设备的激增，加上边界的消失和不断变化的威胁态势，使本来已经很复杂的环境更加复杂，导致企业难以抵御高级攻击者。

攻击既来自企业外部也来自企业内部。而且，随着应用程序向云迁移以及物联网产品的快速采用，企业攻击面持续增加。此外，业务系统、信息技术和运营技术的集成使企业能够从根本上改变业务运营的有效性和效率。

随着这种数字化转型，企业的数字能力越来越重要，因此企业必须将网络安全策略作为优先事项。数字化转型会带来更多可供利用的入口点和盲点，可能会为攻击者带来更多的机会，这使得网络安全专家更难修复所有漏洞和跟踪所有威胁。

不足为奇，随着网络结构的不断扩展，无法识别安全盲点的可能性也会随之增加。因此，企业承受着缩小可见性差距的巨大压力——尤其是在最近的安全事件之后。这导致很多企业以比预期更被动的方式执行网络安全策略。他们不断向安全堆栈中添加单点解决方案，以期立即解决特定安全问题。然而，他们并未详细分析这些单点解决方案能否与其他已存在的安全方案协同工作，或者这些解决方案是否属于重复建设。

通过这种被动的方法，企业无意间引入了更多的安全漏洞，这使得企业难以在所有网络工具中实现可见性，更不用说在整个企业中了。短期修复也是一个难题——对于正在努力应对广泛的网络技能差距，并且不具备自动缓解能力的企业来说，这是最难的部分。而对于没有量身定制的威胁情报或无法执行高级威胁猎杀的企业来说，这些问题会进一步加剧。

攻击者利用这些累积的漏洞来渗透传统的网络防御，并潜伏在盲区，有时长达数周或数月。因此，认识到这些漏洞的企业应如何采取主动、整体的方式来进行修复呢？

首先，安全团队必须具有完全的可见性。“可见性”一词已经被广泛使用，但我认为我们必须为其设置适当的情境。完全的可见性是指考虑到企业内的所有设备以及企业的所有通信，以采取必要的防御措施最大程度地缩短网络攻击在网内的存活时间。企业必须对高价值资产（攻击者最想利用这些资产牟取经济或知识产权利益）进行实时、连续监控。

攻击者将利用阻力最小的路径在企业中横向移动，因此可见性必须涵盖所有托管和非托管资产（企业物联网、影子物联网、老旧系统等）以及相关通信路径。此外，企业必须消除盲点；否则，攻击者将继续利用网络安全防御系统中的漏洞。

其次，对计算机进程和网络活动的可见性，对于检测规则和违规、异常和可疑行为至关重要。重要的防御对策包括：自动检测、威胁猎杀、在数据被盗之前进行响应以调查或自动隔离 / 修复威胁的能力。此外，防御对策还必须涵盖实时防止攻击的技术，包括：签名检测，以隔离端点处的已知不良文件；行为分析，以终止端点处的进程；检测到文件和网络行为后中断网络会话；以及电子邮件隔离。安全团队应根据网络威胁框架调整攻击后的检测和响应措施，以全面覆盖已知攻击面。

第三，了解每个端口的每个通信，这种能力至关重要。企业必须：在整个企业内部署安全解决方案，以收集相关数据；进行流分析以实时处理数据；在关键路口部署响应机制，以降低攻击造成的损失。企业还应该采用机器学习算法来预测攻击者的行动。预测攻击者未来移动的能力，对于遏制横向移动和缩短网络攻击在网内的存活时间至关重要。只有这样，安全团队才能预测下一步攻击并加以隔离。

最后，随着攻击者和恶意内部人员不断发展其策略，试图击败网络安全防御，最好的检测方法不仅要关注他们当前的行动，还要关注他们过去行动的累积影响。安全解决方案必须不断收集和评估元数据（所有通信路径），以发现新的威胁情报。这样能够发现规避网络安全对策的高级威胁。自动化、回顾性分析为分析师提供了更大的可见性，使他们可以回顾系统并深入分析攻击发生时的情况，包括攻击者如何渗透网络安全防御、攻击者执行了什么操作，以及需要采取哪些措施来防止将来攻击等。

只有实时了解安全状况，企业才能充满信心地运作。通常，这些信息是通过为企业各个级别的决策者创建的仪表板传达的。高级管理人员仪表板需要简洁地描述企业的整体安全合规性以及迫在眉睫的威胁的潜在影响。安全团队仪表板需要显示高级、实时事件和威胁，并显示所有详细信息，以便安全团队更快地对事件进行响应以阻止威胁。

连续、实时可见性的另一个重要方面是：允许企业收集和描述其“正常行为”。这一点至关重要，尤其是在尝试识别异常活动（例如内部人员威胁）时。这项工作的最终目标是将传统的被动安全功能转变为更具预测性和主动性的功能，以应对高级持续性威胁（APT）。理想情况下，企业应具备自动响应能力，以便及时做出响应。在这种情况下，仪表板应根据企业安全解决方案的规则和策略，显示操作的摘要信息。

总而言之，为了在无休止的网络战中获得决定性的优势，企业需要对其网络结构具备连续和实时的可见性，并将其作为整体防御策略的主要部分……因为企业无法捍卫看不到的东西。

原文名称	You Can't Defend What You Can't See: Why Visibility is Critical for Improving Cyber Defense
作者简介	Craig Harber。Craig Harber 是 Fidelis Cybersecurity 的首席技术官。
原文信息	2019 年 11 月 12 日发布于 Security Week 原文地址 https://www.securityweek.com/you-cant-defend-what-you-cant-see-why-visibility-critical-improving-cyber-defense
免责声明	本译文译者为安天实验室工程师，出自个人兴趣在业余时间所译，本文原文来自互联网，译者与安天实验室均与原作者与原始发布者没有联系，亦未获得相关的版权授权，鉴于译者及安天实验室出于学习参考之目的翻译本文，而无出版、发售译文等任何商业利益意图，因此亦不对任何可能因此导致的版权问题承担责任。译者力图忠于所获得之电子版本进行翻译，但受翻译水平和技术水平所限，不能完全保证译文完全与原文含义一致，同时对所获得原文是否存在臆造、或者是否与其原始版本一致未进行可靠性验证和评价。译者与安天实验室亦对原文和译文的任何内容不承担任何责任。翻译本文的行为不代表译者和安天实验室对原文立场持有任何立场和态度。 本译文亦不得用于任何商业目的，未授权任何人士和第三方二次分享本译文，基于上述问题产生的法律责任，译者与安天实验室一律不予承担。